KODE SSRS (SUBSPACE SUBCODES OF REED-SOLOMON)

Afifatus Sholihah
Jurusan Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Surabaya,
e-mail: afif165@ymail.com

Agung Lukito
Jurusan Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Surabaya,
e-mail: gung_lukito@yahoo.co.id

Abstrak

Salah satu kelas kode siklik nonlinier adalah Kode SSRS (*Subspace Subcodes of Reed-Solomon*). Kode SSRS merupakan subset kode RS (*Reed-Solomon*) atas $GF(2^m)$ yang semua komponen katakodenya berada di subruang $GF(2^m)$ berdimensi v. Kode SSRS tidak linier atas $GF(2^v)$ tetapi linier atas $GF(2)$. Banyaknya katakode di kode SSRS adalah $2^{K(\mathbb{C},S)}$, dengan $K(\mathbb{C},S)$ adalah dimensi kode SSRS atas $GF(2)$.

Kata kunci: Kode SSRS, kelas kode Reed-Solomon, dan kode nonbiner.

Abstract

One of class of nonlinear cyclic codes is SSRS (*Subspace Subcodes of Reed-Solomon*) codes. SSRS codes are a subset of RS (*Reed-Solomon*) codes over $GF(2^m)$ whose components are all of the RS codewords that lie in v-dimensional vector subspace of $GF(2^m)$. They are not linear over $GF(2^v)$ but linear over $GF(2)$. The number of codewords in a SSRS code is $2^{K(\mathbb{C},S)}$, with $K(\mathbb{C},S)$ is the dimension of SSRS codes over $GF(2)$.

Keywords: SSRS codes, class of Reed-Solomon codes, and nonbinary codes.

1. PENDAHULUAN

1.1 Latar Belakang

Kode RS (*Reed-Solomon*) adalah salah satu kode yang mampu mengoreksi banyak kesalahan (*multiple error*). Karena keunggulannya dalam mendeteksi dan mengoreksi kesalahan, maka kode RS ini banyak digunakan dalam sistem telekomunikasi.

Salah satu kelas kode RS adalah kode SSRS. Kode SSRS merupakan kode RS atas $GF(2^m)$ yang semua komponennya berada pada subruang $GF(2^m)$. Misalkan S adalah subruang $GF(2^m)$ yang berdimensi v, maka kode SSRS tidak linier atas $GF(2^v)$. Karena ketidaklinieran kode SSRS atas $GF(2^v)$, maka kode SRS merupakan salah satu kelas kode nonlinier.

Karena kode SSRS adalah kode nonlinier, maka untuk menghitung banyak katakode di kode SSRS kita harus mendaftar satu per satu katakode di kode SSRS. Jika nilai n (panjang katakode) besar, maka kita akan kesulitan mendaftar katakode di kode SSRS, sehingga pada makalah ini dibahas bagaimana mengetahui banyaknya katakode di kode SSRS tanpa mendaftar katakode di kode SSRS satu per satu, yaitu menggunakan teorema yang menyatakan dimensi biner kode SSRS yang penulis ambil dari jurnal Hattori Mayasuki, Robbert J. McEliece dan Gustave Solomon yang berjudul *Subspace Subcodes of Reed-Solomon Codes*.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas maka rumusan masalah dalam makalah ini adalah berapa banyak katakode di kode SSRS.

1.3 Tujuan Penulisan

Berdasarkan rumusan masalah di atas, tujuan penulisan makalah adalah mengetahui banyaknya katakode di kode SSRS.

1.4 Batasan Masalah

Pada makalah ini tidak dibahas dekoding kode SSRS dan kode SSRS yang dibahas adalah kode SSRS atas $GF(2^m)$. Larik yang dimaksud pada makalah ini adalah *array*.

1.5 Manfaat Penulisan

Adapun manfaat dari penulisan makalah ini antara lain:

a. Bagi penulis, sebagai tambahan informasi dan wawasan mengenai kode SSRS.
b. Bagi pengguna matematika, sebagai tambahan pengetahuan bidang matematika, khususnya bidang pengkodean.

1.6 Metode Penulisan

Metode yang digunakan di sini adalah metode kajian pustaka. Adapun langkah-langkah dalam penulisan makalah ini adalah :

a. Mengumpulkan informasi yang berhubungan dengan materi terkait serta membaca, memahami dan menelaah beberapa buku dan referensi lain, seperti jurnal ilmiah, hasil penelitian terdahulu, dan lain-lain.
b. Menuliskannya ke dalam bentuk makalah.

2. HASIL DAN PEMBAHASAN

Pada bab ini akan dibahas definisi formal kode SSRS serta konjugat lapangan, trace, subruang trace-dual, konjugat modulo n, koset siklotomik modulo n, larik sikltomik modulo n, dan matriks siklotomik modulo n yang digunakan untuk menghitung dimensi biner kode SSRS. Selain itu, dibahas teorema yang menyatakan dimensi biner kode SSRS yang digunakan untuk menghitung banyaknya katakode di kode SSRS dan beberapa lemma dan teorema yang berhubungan dengan kode SSRS serta akan diberikan contoh bagaimana menggunakan teorema dimensi biner kode SSRS untuk menghitung banyak katakode di kode SRSS jika diberikan kode RS atas $GF(2^m)$ dan subruang $GF(2^m)$.

2.1 KONJUGAT, TRACE, DAN SUBRUANG TRACE-DUAL

Definisi 2.1.1 (Konjugat) Misalkan $GF(p^m)$ perluasan lapangan $GF(p)$ dan $\alpha \in GF(p^m)$. $\alpha, \alpha^p, \alpha^{p^2}, \dots, \alpha^{p^{m-1}}$ disebut konjugat α.

Definisi 2.1.2 (Trace) Misalkan $\alpha \in GF(p^m)$. Trace α atas $GF(p^d)$, dinotasikan dengan $Tr_d^m(\alpha)$, didefinisikan dengan:

$$Tr_d^m(\alpha) = \alpha + \alpha^{p^d} + \alpha^{p^{2d}} + \cdots + \alpha^{p^{(f-1)d}}, \qquad (2.1.1)$$

dengan $d|m$ dan $f = \frac{m}{d}$.

Contoh 2.1.1

Diberikan $GF(2^4)$ sebagai berikut:

Misalkan $\langle x^4 + x + 1\rangle = I$, maka

$$GF(2^4) = \mathbb{Z}_2[x]/\langle x^4 + x + 1\rangle$$
$$= \{I, I+1, I+x, I+(1+x), I+x^2, I+(1+x^2), I+(x+x^2), I+(1+x+x^2), I+x^3, I+(1+x^3), I+(x+x^3), I+(x^2+x^3), I+(1+x+x^3), I+(1+x^2+x^3), I+(x+x^2+x^3), I+(1+x+x^2+x^3)\}.$$

Elemen tak nol $\alpha = I + x$ adalah elemen primitif $GF(2^4)$, sehingga diperoleh:

$\alpha^0 = I + 1$ $\quad$ $\alpha^8 = I + (1 + x^2)$
$\alpha^1 = I + x$ $\quad$ $\alpha^9 = I + (x + x^3)$
$\alpha^2 = I + x^2$ $\quad$ $\alpha^{10} = I + (1 + x + x^2)$
$\alpha^3 = I + x^3$ $\quad$ $\alpha^{11} = I + (x + x^2 + x^3)$
$\alpha^4 = I + (1 + x)$ $\quad$ $\alpha^{12} = I + (1 + x + x^2 + x^3)$
$\alpha^5 = I + (x + x^2)$ $\quad$ $\alpha^{13} = I + (1 + x^2 + x^3)$
$\alpha^6 = I + (x^2 + x^3)$ $\quad$ $\alpha^{14} = I + (1 + x^3)$
$\alpha^7 = I + (1 + x + x^3)$

Jika elemen lapangan $a_0 + a_1x + a_2x^2 + a_3x^3$ disajikan dalam bentuk 4-tupel $(a_0a_1a_2a_3)$ dengan mengurutkan dari pangkat terkecil ke pangkat yang besar, maka dengan penyajian tersebut, elemen $GF(2^4)$ adalah:

$\alpha^0 = 1000$ $\quad$ $\alpha^8 = 1010$
$\alpha^1 = 0100$ $\quad$ $\alpha^9 = 0101$
$\alpha^2 = 0010$ $\quad$ $\alpha^{10} = 1110$
$\alpha^3 = 0001$ $\quad$ $\alpha^{11} = 0111$
$\alpha^4 = 1100$ $\quad$ $\alpha^{12} = 1111$
$\alpha^5 = 0110$ $\quad$ $\alpha^{13} = 1011$
$\alpha^6 = 0011$ $\quad$ $\alpha^{14} = 1001$
$\alpha^7 = 1101$

Konjugat $\alpha^3 = 0001$adalah
$\alpha^3 = 0001$
$(\alpha^3)^2 = \alpha^6 = 0011$
$(\alpha^3)^{2^2} = \alpha^{12} = 1111$
$(\alpha^3)^{2^3} = \alpha^9 = 0101$,
dan $Tr_1^4(\alpha^3)$ adalah 1000.

Teorema 2.1.1

Jika $d|m$, maka $Tr_1^m(x) = Tr_1^d\left(Tr_d^m(x)\right)$.

Bukti:

Misalkan $f = \frac{m}{d}$.

$$Tr_1^d\left(Tr_d^m(x)\right) = Tr_1^d\left(x + x^{p^d} + \cdots + x^{p^{(f-1)d}}\right)$$
$$= \left(x + x^{p^d} + \cdots + x^{p^{(f-1)d}}\right) + \left(x + x^{p^d} + \cdots + x^{p^{(f-1)d}}\right)^p + \left(x + x^{p^d} + \cdots + x^{p^{(f-1)d}}\right)^{p^2} + \cdots + \left(x + x^{p^d} + \cdots + x^{p^{(f-1)d}}\right)^{p^{d-1}}$$
$$= \left(x + x^{p^d} + \cdots + x^{p^{(f-1)d}}\right) + \left(x^p + x^{p^{d+1}} + \cdots + x^{p^{(f-1)d+1}}\right) + \left(x^{p^2} + x^{p^{d+2}} + \cdots + x^{p^{(f-1)d+2}}\right) + \cdots + \left(x^{p^{d-1}} + x^{p^{2d-1}} + \cdots + x^{p^{fd-1}}\right)$$
$$= x + x^p + x^{p^2} + \cdots + x^{p^{d-1}} + x^{p^d} + x^{p^{d+1}} + x^{p^{d+2}} + \cdots + x^{p^{2d-1}} + \cdots +$$

$$x^{p^{(f-1)d}} + x^{p^{(f-1)d+1}} + x^{p^{(f-1)d+2}} + \cdots + x^{p^{fd-1}}$$
$$= x + x^p + x^{p^2} + \cdots + x^{p^{fd-1}}$$
$$= x + x^p + x^{p^2} + \cdots + x^{p^{m-1}}$$
$$= Tr_1^m(x). \quad \blacksquare$$

Definisi 2.1.3 (Basis dual)
Diberikan $A = \{\alpha_0, \alpha_1, \dots, \alpha_{m-1}\}$ adalah basis untuk $GF(2^m)$, basis dual untuk A adalah $B = \{\beta_0, \beta_1, \dots, \beta_{m-1}\} \subseteq GF(2^m)$ dengan

$$Tr_1^m(\alpha_i.\beta_j) = \begin{cases} 1, i = j \\ 0, i \neq j. \end{cases} \quad (2.1.2)$$

Dalam [13, hal. 110] dijelaskan bagaimana menentukan basis dual ini:

1. definisikan matriks persegi A atas $GF(2)$ dengan ordo $m \times m$ dengan $A = \left(a_{ij}\right)_{i,j=0}^{m-1}$ dan $a_{ij} = Tr_1^m(\alpha_i\alpha_j)$,
2. misalkan $B = A^{-1}$ maka jika entri (k, j) matriks B dinotasikan dengan b_{kj} maka basis dualnya adalah

$$\beta_j = \sum_{k=0}^{m-1} b_{kj}\alpha_k, \quad j = 0,1, \dots, m-1.$$

Jika $x \in GF(2^m)$, maka x dapat dinyatakan sebagai kombinasi linier basis yaitu:

$$x = \sum_{j=0}^{m-1} z_j\alpha_j, \qquad z_j \in GF(2),$$

z_j disebut komponen biner ke-j dari x yang ditentukan dengan

$$z_j = Tr_1^m(x\beta_j), \qquad j = 0,1, \dots, m-1. \quad (2.1.3)$$

Dalam [13, hal. 110] juga dijelaskan basis dual selalu ada dan tunggal.

Contoh 2.1.2
Basis untuk $GF(2^4)$ pada contoh 2.1.1 adalah $\{1, \alpha, \alpha^2, \alpha^3\}$, sehingga diperoleh matriks A dan B sebagai berikut:

$$A = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

Basis dual untuk $\{1, \alpha, \alpha^2, \alpha^3\}$ adalah $\beta_0 = 1 + \alpha^3 = \alpha^{14}$, $\beta_1 = \alpha^2$, $\beta_2 = \alpha$, dan $\beta_3 = 1$.

Definisi 2.1.4 (Subruang Trace-Dual)
Misalkan S subruang berdimensi v dari $GF(2^m)$. Subruang trace-dual untuk S, yang dinotasikan dengan $S^\perp$, adalah subruang berdimensi μ dari $GF(2^m)$ dengan $\mu = m - v$ sedemikian hingga $\forall x \in S$ dan $\forall y \in S^\perp$ berlaku :

$$Tr_1^m(xy) = 0 \begin{cases} \forall x \in S \\ \forall y \in S^\perp. \end{cases} \quad (2.1.4)$$

Basis yang merentang subruang trace-dual disebut basis trace-dual.

Contoh 2.1.3

Basis yang merentang $GF(2^4)$ adalah $A = \{1, \alpha, \alpha^2, \alpha^3\}$. Kemudian diberikan $S_1 = \{0, \alpha^0, \alpha, \alpha^4\}$, $S_2 = GF(2^4)$ dan $S_3 = \{0, \alpha^0, \alpha, \alpha^2, \alpha^4, \alpha^5, \alpha^8, \alpha^{10}\}$ adalah subruang $GF(2^4)$ yang masing-masing subruang secara berurutan direntang basis $B_1 = \{1, \alpha\}, B_2 = \{1, \alpha, \alpha^2, \alpha^3\}$ dan $B_3 = \{1, \alpha, \alpha^2\}$, maka $S_1^\perp = S$, $S_2^\perp = \{0\}$ dan $S_3^\perp = \{0, \alpha^0\}$.

2.2 KONJUGAT MODULO n DAN KOSET SIKLOTOMIK MODULO n

Definisi 2.2.1 (Konjugat Modulo n)
Diberikan n adalah bilangan bulat positif ganjil dan m adalah bilangan bulat positif terkecil sedemikian hingga $n|2^m - 1$. Jika i dan j adalah bilangan bulat dengan $0 \leq i \leq n-1$ dan $0 \leq j \leq n-1$, maka i dan j disebut konjugat modulo n jika dan hanya jika $\exists s \in \mathbb{Z} \ni 2^s i \equiv j(mod\ n)$.

Contoh 2.2.1
Diberikan $n = 15$. Bilangan bulat positif terkecil m yang memenuhi $15|2^m - 1$ adalah $m = 4$. Untuk $i = j = 3$ merupakan konjugat modulo 15 karena $\exists s = 0 \ni 2^0.3 \equiv 3(mod\ 15)$. Sedangkan untuk $i \neq j$ dengan $j = 3$, ada 9 dan 3, 12 dan 3, 6 dan 3 juga merupakan konjugat modulo 15 karena ada s sedemikian hingga

$$2^1.9 \equiv 3(mod\ 15)$$
$$2^2.12 \equiv 3(mod\ 15)$$
$$2^3.6 \equiv 3(mod\ 15).$$

Teorema 2.2.1
Konjugasi modulo n adalah relasi ekuivalensi pada himpunan bilangan bulat
Bukti:
Akan ditunjukkan konjugasi modulo n memenuhi sifat refleksif, simetris, dan transitif.
1) (Refleksif) $a \equiv a(mod\ n)$
Ambil sebarang $a \in \mathbb{Z}$ dengan $0 \leq a \leq n-1$. a dan a adalah konjugat modulo n, karena ada $s = 0$ sedemikian hingga $2^0 a = a \equiv a(mod\ n)$.

2) (Simetris) $2^s a \equiv b(mod\ n) \rightarrow 2^t b \equiv a(mod\ n)$
Ambil sebarang $a, b \in \mathbb{Z}$ dengan $0 \leq a \leq n-1$, $0 \leq b \leq n-1$, dan

$$2^s a \equiv b(mod\ n).$$

Kedua ruas dikalikan 2^{m-s} dan diperoleh:

$$2^{m-s}2^s a \equiv 2^{m-s}b(mod\ n)$$
$$2^m a \equiv 2^{m-s}b(mod\ n).$$

Karena m adalah bilangan bulat terkecil yang memenuhi $n|2^m - 1$, $n|2^m - 1 \leftrightarrow 2^m \equiv 1(mod\ n)$. Jadi,

$$1a \equiv 2^{m-s}b(mod\ n)$$
$$a \equiv 2^{m-s}b(mod\ n)$$
$$2^{m-s}b \equiv a(mod\ n).$$

Karena ada $t = m - s$ sedemikian hingga $2^t b \equiv a(mod\ n)$, maka b dan a konjugat modulo n.

3) (Transitif) $2^s a \equiv b(mod\ n)$ dan $2^t b \equiv c(mod\ n) \rightarrow 2^u a \equiv c(mod\ n)$
Ambil sebarang $a, b, c \in \mathbb{Z}$ dengan $0 \leq a \leq n-1$, $0 \leq b \leq n-1$, $0 \leq c \leq n-1$, dan

$2^s a \equiv b(mod\ n)$ (2.2.1)

$2^t b \equiv c(mod\ n)$. (2.2.2)

Dari (2.2.1) dan (2.2.2) diperoleh $2^s a - b = k_1 n, \exists k_1 \in \mathbb{Z}$ dan $2^t b - c = k_2 n,\ \exists k_2 \in \mathbb{Z}$. Dengan menggantikan $b = 2^s a - k_1 n$ ke (2.2.2), diperoleh

$$2^t(2^s a - k_1 n) - c = k_2 n$$
$$2^{t+s} a - 2^t k_1 n - c = k_2 n$$
$$2^{t+s} a - c = k_2 n + 2^t k_1 n$$
$$2^{t+s} a - c = (k_2 + 2^t k_1) n. \quad (2.2.3)$$

Dari (2.2.3), diperoleh $2^{t+s} a \equiv c\ (mod\ n)$. Karena ada $u = t + s$ sedemikian hingga $2^u a \equiv c(mod\ n)$, maka a dan c konjugat modulo n.

Dari 1), 2), dan 3) terbukti bahwa konjugasi modulo n adalah relasi ekuivalensi.■

Karena konjugasi modulo n merupakan relasi ekuivalensi maka diperoleh kelas-kelas ekuivalensi.

Definisi 2.2.2 (Koset Siklotomik modulo n)
Kelas-kelas ekuivalensi pada relasi konjugasi modulo n disebut koset siklotomik modulo n.

Jika $j \in \mathbb{Z}_n$, maka koset siklotomik yang memuat j dapat dinyatakan sebagai himpunan $\{j, 2j, \dots, 2^{d-1}j\}$ yang dinotasikan dengan Ω_j, dengan d adalah bilangan bulat positif terkecil yang memenuhi $2^d j \equiv j(mod\ n)$, dan d disebut dengan derajat j, yang dinotasikan dengan $d = \deg(j)$.
Untuk selanjutnya didefinisikan $f_j = \frac{m}{d_j}$ dan I_n adalah himpunan semua bilangan bulat terkecil pada setiap koset siklotomik modulo n.

Contoh 2.2.2
Koset siklotomik modulo 15 dapat dinyatakan sebagai himpunan $\{j, 2j, \dots, 2^{d-1}j\}$ yang dinotasikan dengan Ω_j, dengan $0 \le j \le 14$. Bilangan bulat positif m yang memenuhi $15|2^m - 1$ adalah $m = 4$. Kemudian, dicari bilangan bulat positif terkecil d yang memenuhi $2^d j \equiv j(mod\ n)$, dengan $0 \le j \le 14$.
Untuk $j = 0$, bilangan bulat positif d_0 yang memenuhi $2^{d_0} 0 \equiv 0(mod\ 15)$ adalah $d_0 = 1$, sehingga $\Omega_0 = \{0\}$ dan $f_0 = 1$.
Untuk $j = 1$, bilangan bulat positif d_1 yang memenuhi $2^{d_1} 1 \equiv 1(mod\ 15)$ adalah $d_1 = 4$, sehingga $\Omega_1 = \{1,2,4,8\}$ dan $f_1 = 1$.
Dengan cara yang sama, diperoleh d_j dan f_j untuk $j \in I_{15} = \{0,1,3,5,7\}$ adalah:

$\Omega_0 = \{0\}$	$d_0 = 1$	$f_0 = 4$
$\Omega_1 = \{1,2,4,8\}$	$d_1 = 4$	$f_1 = 1$
$\Omega_3 = \{3,6,12,9\}$	$d_3 = 4$	$f_3 = 1$
$\Omega_5 = \{5,10\}$	$d_5 = 2$	$f_5 = 2$
$\Omega_7 = \{7,14,13,11\}$	$d_7 = 4$	$f_7 = 1$

Definisi 2.2.3 (Larik Siklotomik modulo n)
Larik siklotomik modulo n adalah larik bilangan bulat dengan $|I_n|$ baris dan m kolom, yang baris ke- j berkorespondensi dengan koset siklotomik ke-j.

Karena itu, larik siklotomik modulo n merupakan matriks bilangan bulat berordo $|I_n| \times m$ yang entri-entrinya adalah bilangan bulat modulo n dan entri ke- $(j,i) = j2^i(mod\ n)$ dengan $j \in I_n$ dan $i \in \{0,1,\dots,n-1\}$.

Contoh 2.2.3
Dari contoh 2.2.2 dapat dibentuk larik siklotomik modulo 15 sebagai berikut:

	Index i					
	0	1	2	3		
$j = 0$	0	0	0	0	$d_0 = 1$	$f_0 = 4$
$j = 1$	1	2	4	8	$d_1 = 4$	$f_1 = 1$
$j = 3$	3	6	12	9	$d_3 = 4$	$f_3 = 1$
$j = 5$	5	10	5	10	$d_5 = 2$	$f_5 = 2$
$j = 7$	7	14	13	11	$d_7 = 4$	$f_7 = 1$

2.3 MATRIKS SIKLOTOMIK MODULO n

Misalkan S adalah subruang dari $GF(2^m)$ atas $GF(2)$ yang berdimensi v dan basis trace-dual yang merentang subruang trace-dual $S^\perp$ adalah $\{\gamma_0, \gamma_1, \dots, \gamma_{\mu-1}\}$.

Definisi 2.3.1 (Matriks Siklotomik)
Diberikan himpunan J dan koset siklotomik modulo n. Himpunan J adalah himpunan bilangan bulat yang elemennya dipilih dari $\{0,1,\dots,n-1\}$ yang membentuk barisan aritmatika modulo n yang bedanya prima relatif dengan n. Kemudian, didefinisikan $J_j = J \cap \Omega_j$ untuk setiap $j \in I_n$. Misalkan $e_j = |J_j|$ adalah banyaknya elemen J_j dan A_j adalah himpunan bilangan bulat i yang memenuhi $j2^i\ mod\ n \in J_j$ dengan $0 \le i \le m-1$, maka $|A_j| = a_j = e_j f_j$, dengan

$$A_j = \left\{i_0, i_1, \dots, i_{a_j-1}\right\},\ i_0 < i_1 < \cdots < i_{a_j-1}. \quad (2.3.1)$$

Matriks siklotomik ke-j, yang dinotasikan dengan Γ_j, yang terkait dengan Ω_j didefinisikan sebagai matriks dengan ordo $\mu \times a_j$ yang berbentuk:

$$\Gamma_j = \begin{bmatrix} \gamma_0^{2^{m-i_0}} & \gamma_0^{2^{m-i_1}} & \cdots & \gamma_0^{2^{m-i_{a_j-1}}} \\ \gamma_1^{2^{m-i_0}} & \gamma_1^{2^{m-i_1}} & & \gamma_0^{2^{m-i_{a_j-1}}} \\ \vdots & & \ddots & \vdots \\ \gamma_{\mu-1}^{2^{m-i_0}} & \gamma_{\mu-1}^{2^{m-i_1}} & \cdots & \gamma_{\mu-1}^{2^{m-i_{a_j-1}}} \end{bmatrix}, \quad (2.3.2)$$

dengan $\{\gamma_0, \gamma_1, \dots, \gamma_{\mu-1}\}$ adalah basis trace-dual.

Contoh 2.3.1
Diberikan subruang $GF(2^4)$ adalah $S = \{0, \alpha^0, \alpha, \alpha^4\}$. Subruang trace-dual untuk $S^\perp = S$. Kemudian diberikan $J = \{1,2,3,4,5,6,7,8,9\}$ dan koset siklotomik modulo 15 pada contoh 2.2.2, sehingga diperoleh $I_{15} = \{0,1,3,5,7\}$ dan larik siklotomik modulo 15 adalah:

	Index i						
	0	1	2	3			
$j = 0$	0	0	0	0	$e_0 = 0$	$A_0 = \emptyset$	$a_0 = 0$

$j=1$	**1**	**2**	**4**	**8**	$e_1=4$	$A_1=\{0,1,2,3\}$
$j=3$	**3**	**6**	12	**9**	$e_3=3$	$A_3=\{0,1,3\}$
$j=5$	**5**	10	**5**	10	$e_5=1$	$A_5=\{0,2\}$
$j=7$	**7**	14	13	11	$e_7=1$	$A_7=\{0\}$

Sehingga matriks siklotomik untuk S adalah:

$$\Gamma_1=\begin{bmatrix}1 & 1 & 1 & 1\\ \alpha & \alpha^8 & \alpha^4 & \alpha^2\end{bmatrix}.$$
$$\Gamma_3=\begin{bmatrix}1 & 1 & 1\\ \alpha & \alpha^8 & \alpha^2\end{bmatrix}$$
$$\Gamma_5=\begin{bmatrix}1 & 1\\ \alpha & \alpha^4\end{bmatrix}$$
$$\Gamma_7=\begin{bmatrix}1\\ \alpha\end{bmatrix}.$$

2.4 KODE SSRS

Diberikan lapangan $GF(2^m)$, bilangan bulat positif ganjil n dengan $n|2^m-1$, akar ke-n kesatuan primitif di $GF(2^m)$, misalkan α, dan himpunan J. Himpunan J adalah himpunan k_0 bilangan bulat yang elemennya dipilih dari $\{0,1,\dots,n-1\}$ yang membentuk barisan aritmatika modulo n yang bedanya prima relatif dengan n. Kemudian didefinisikan $\mathbb{C}(J)$ adalah kode RS dengan parameter (n,k_0,d_0) atas $GF(2^m)$, dengan polinomial cek paritas $h(x)$ dan polinomial pembangkit $g(x)$ sebagai berikut:

$$h(x)=\prod_{j\in J}(x-\alpha^j) \qquad (2.4.1)$$

$$g(x)=\prod_{j\in \bar{J}}(x-\alpha^j), \qquad (2.4.2)$$

dengan $\bar{J}$ adalah himpunan $n-k_0$ bilangan bulat yang membentuk komplemen J sedemikian hingga $x^n-1=g(x)h(x)$.

Karena $\mathbb{C}(J)$ merupakan kode RS atas $GF(2^m)$ dengan parameter (n,k_0,d_0), maka $\mathbb{C}(J)$ terdiri atas semua vektor $\boldsymbol{\mathcal{C}}=(\mathcal{C}_0,\mathcal{C}_1,\dots,\mathcal{C}_{n-1})$ dengan $\mathcal{C}_i\in GF(2^m)$. Jika $\boldsymbol{\mathcal{C}}$ dinyatakan dalam polinomial, maka $\mathcal{C}_i$ adalah koefisien–koefisien pada polinomial tersebut. Dengan menggunakan polinomial Mattson-Solomon $P(x)$ diperoleh:

$$\mathcal{C}_i=P(\alpha^i), \qquad i=0,1,\dots,n-1, \qquad (2.4.3)$$

dengan

$$P(x)=\sum_{j\in J}c_j x^j, \quad \forall c_j\in GF(2^m). \qquad (2.4.4)$$

Untuk selanjutnya, jika diberikan himpunan J, maka himpunan J adalah himpunan k_0 bilangan bulat yang elemennya dipilih dari $\{0,1,\dots,n-1\}$ yang membentuk barisan aritmatika modulo n yang bedanya prima relatif dengan n. Dan himpunan yang elemen-elemennya adalah c_j untuk $j\in J$ dinotasikan dengan C_j.

Definisi 2.4.1 (Definisi Formal Kode SSRS)
Diberikan $\mathbb{C}$ (n,k_0,d_0) adalah kode siklik RS atas $GF(2^m)$ dan S adalah subruang dari $GF(2^m)$ berdimensi v. *Subspace subcode* yang terkait dengan $\mathbb{C}$ dan S, yang dinotasikan dengan $\mathbb{C}_S$, didefinisikan sebagai himpunan katakode $\mathbb{C}$ yang semua komponennya berada di S.

Contoh 2.4.1
Diberikan $\mathbb{C}$ adalah kode RS atas $GF(2^4)$ dengan parameter $(5,3,3)$ dan $S=\{0,\alpha^0,\alpha,\alpha^4,\alpha^6,\alpha^{11},\alpha^{13}\}$ adalah subruang $GF(2^4)$ atas $GF(2)$ yang direntang basis $\{\alpha^0,\alpha,\alpha^6\}$. Kode $\mathbb{C}_S$ adalah kode $\mathbb{C}$ yang semua komponennya berada di S. Salah satu katakode di $\mathbb{C}_S$ adalah $\alpha^4\alpha^{13}\alpha^6\alpha^{13}\alpha^{11}$ yang merupakan kode RS atas $GF(2^4)$ dengan:

$$h(x)=(x-\alpha)(x-\alpha^2)(x-\alpha^3)$$
$$=x^3+\alpha^{11}x^2+\alpha^{13}x+\alpha^6$$
$$g(x)=(x-\alpha^0)(x-\alpha^4)=x^2+\alpha x+\alpha^4.$$

Kode $\mathbb{C}_S$ kode nonlinier atas $GF(2^v)$ sehingga banyaknya katakode di $\mathbb{C}_S$ tidak selalu perpangkatan 2^v. Akan tetapi, $\mathbb{C}_S$ adalah kode linier atas $GF(2)$ sehingga untuk menentukan banyak katakode di $\mathbb{C}_S$ bisa menggunakan sifat $\mathbb{C}_S$ yang merupakan kode linier atas $GF(2)$. Karena $\mathbb{C}_S$ kode linier atas $GF(2)$, maka banyaknya katakode di $\mathbb{C}_S$ adalah perpangkatan 2.

Misalkan dimensi $\mathbb{C}_S$ atas $GF(2)$ adalah $K(\mathbb{C},S)$ dan $|\mathbb{C}_S|$ adalah banyaknya katakode di $\mathbb{C}_S$, maka

$$|\mathbb{C}_S|=2^{K(\mathbb{C},S)}, \qquad (2.4.5)$$

dan dimensi untuk $\mathbb{C}_S$ atas S adalah:

$$k(\mathbb{C},S)=\frac{1}{v}K(\mathbb{C},S)=\frac{|S|}{v}\log|\mathbb{C}_S|. \qquad (2.4.6)$$

2.5 DIMENSI KODE SSRS

Diberikan $P(x)$ adalah polinomial atas $GF(2^m)$ yang berderajat $n-1$ dengan $n|2^m-1$, maka

$$P(x)=\sum_{j=0}^{n-1}P_j x^j, \quad P_j\in GF(2^m). \qquad (2.5.1)$$

Kemudian, didefinisikan polinomial $\mathcal{P}(x)$ sebagai berikut:

$$\mathcal{P}(x)=Tr_1^m\big(P(x)\big)\ mod\ (x^n-1) \qquad (2.5.2)$$

$$=\sum_{j=0}^{n-1}\mathcal{P}_j x^j \qquad (2.5.3)$$

Lemma 2.5.1
Diberikan $P(x)$ yang didefinisikan oleh (2.5.1) dan $\mathcal{P}(x)$ oleh (2.5.2) dan (2.5.3). Misalkan α adalah akar ke-n kesatuan primitif di $GF(2^m)$, maka $Tr_1^m\big(P(x)\big)=0$ untuk $x\in\{1,\alpha,\alpha^2,\dots,\alpha^{n-1}\}$ jika dan hanya jika $\mathcal{P}_j=0$ untuk $j=0,1,\dots,n-1$.

Bukti:

($\leftarrow$) Karena $\mathcal{P}_j=0$ untuk $j=0,1,\dots,n-1$, maka $\mathcal{P}(x)=0$ sehingga

$$\mathcal{P}(x)=0=Tr_1^m\big(P(x)\big)\ mod\ (x^n-1). \qquad (*)$$

Dari $(*)$ diperoleh $x^n - 1 | Tr_1^m(P(x))$. Karena α adalah akar ke-n kesatuan primitif di $GF(2^m)$, maka $x^n = 1$ untuk $x \in \{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$, sehingga $x^n - 1 | Tr_1^m(P(x)) = 0 | Tr_1^m(P(x))$. Karena $0 | Tr_1^m(P(x))$, maka $Tr_1^m(P(x)) = 0$ untuk $x \in \{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$.

$(\rightarrow)$ Karena $Tr_1^m(P(x)) = 0$ untuk $x \in \{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$, maka diketahui $\mathcal{P}(x)$ mempunyai n akar yang berbeda. Karena $\mathcal{P}(x)$ berderajat $n-1$, maka $\mathcal{P}(x)$ mempunyai paling banyak $n-1$ akar yang berbeda di sebarang lapangan perluasan $GF(2)$, sehingga $\mathcal{P}(x)$ adalah polinomial nol yang koefisien – koefisiennya adalah nol untuk $j = 0,1, \dots, n-1$. ■

Lemma 2.5.2

Diberikan $P(x)$ yang didefinisikan oleh (2.5.1) dan $\mathcal{P}(x)$ oleh (2.5.2) dan (2.5.3). Jika $d = deg(j)$ untuk $j \in \{0,1,2, \dots, n-1\}$, maka

$$\mathcal{P}_j = \sum_{i=0}^{m-1} P_{2^i j}^{2^{m-i}},$$

dengan m adalah bilangan bulat positif terkecil yang memenuhi $n | 2^m - 1$ dan $2^i j$, 2^{m-i} dalam modulo n.

Bukti:

Karena $\mathcal{P}_j$ adalah koefisien x^j di $\mathcal{P}(x)$, maka untuk menentukan $\mathcal{P}_j$ digunakan $\mathcal{P}(x)$ yang didefinisikan sebagai:

$$\mathcal{P}(x) = Tr_1^m(P(x)) \bmod (x^n - 1). \quad (2.5.4)$$

Karena $P(x) = \sum_{g=0}^{n-1} P_g x^g$, maka

$$\begin{aligned}\mathcal{P}(x) &= Tr_1^m(P(x)) \bmod (x^n - 1)\\ &= \sum_{g=0}^{n-1} Tr_1^m(P_g x^g) \bmod (x^n - 1)\\ &= \sum_{g=0}^{n-1} (P_g x^g) + (P_g x^g)^2 + \cdots \\ &\qquad + (P_g x^g)^{2^{m-1}} \bmod (x^n - 1)\\ &= \sum_{g=0}^{n-1} (P_g x^g) + (P_g^2 x^{2g}) + \cdots \\ &\qquad + (P_g^{2^{m-1}} x^{2^{m-1} g}) \bmod (x^n - 1). \end{aligned} \quad (2.5.5)$$

Karena pangkat yang muncul pada ekspansi $Tr_1^m(P_g x^g)$ adalah konjugat g modulo n; yaitu, $g, 2g, \dots, 2^{m-1}g$, maka untuk $k \in \{g, 2g, \dots, 2^{m-1}g\}$ berlaku $x^k \bmod (x^n - 1) = x^g$, sehingga untuk $g \in \Omega_j$, $\mathcal{P}_j$ di $\mathcal{P}(x)$ adalah koefisien x^g di $\mathcal{P}(x)$.

Dari (2.5.5) diperoleh suku polinomial $\mathcal{P}(x)$ dengan pangkat g dan $\in \Omega_j$, $\mathcal{P}_j(x)$, sebagai berikut:

$$\mathcal{P}_j(x) = (P_g + P_g^2 + P_g^{2^2} + \cdots + P_g^{2^{m-1}}) x^g,$$

sehingga

$$\begin{aligned}\mathcal{P}_j &= P_g + P_g^2 + P_g^{2^2} + \cdots + P_g^{2^{m-1}}\\ &= \sum_{l=0}^{m-1} P_{g,}^{2^l} \end{aligned} \quad (2.5.6)$$

dengan 2^l dan g dalam modulo n.

Karena $n | 2^m - 1$, maka $2^m j \equiv j \ (mod\ n)$, $\quad (2.5.7)$

Sehingga ada d sedemikian hingga $m = d$ untuk $j \in \{0,1,2, \dots, n-1\}$.

Karena $d = deg(j)$, maka untuk setiap $g \in \Omega_j$, ada bilangan bulat i dengan $i \in \{0,1, \dots, d-1\}$ sedemikian hingga $2^i g \bmod n = j$, sehingga $2^i g \equiv j (mod\ n)$. Karena konjugasi modulo n bersifat simetris, maka berdasarkan teorema 3.2.1 ada $t = m - i$ sedemikian hingga $2^t j \equiv g (mod\ n)$ atau dapat ditulis $2^t j \bmod n = g$. Berdasarkan (2.5.7), maka $i \in \{0,1, \dots, m-1\}$ juga memenuhi $2^i g \bmod n = j$. Dengan mengganti $g = 2^t j = 2^{m-i} j$ dan l dengan $i \in \{0,1, \dots, m-1\}$, maka diperoleh:

$$\mathcal{P}_j = \sum_{i=0}^{m-1} P_{2^{m-i} j.}^{2^i} \quad (2.5.8)$$

Karena

$$\begin{aligned} 2^i (2^{m-i} j) \bmod n &= j\\ 2^{m-i} (2^i j) \bmod n &= j, \end{aligned}$$

maka

$$\mathcal{P}_j = \sum_{i=0}^{m-1} P_{2^i j,}^{2^{m-i}} \quad (2.5.9)$$

dengan 2^{m-i} dan $2^i j$ dalam modulo n. ■

Lemma 2.5.3

Jika j_1 dan j_2 adalah konjugat modulo n maka $\mathcal{P}_{j_1}$ dan $\mathcal{P}_{j_2}$ adalah konjugat di $GF(2^m)$.

Bukti:

Karena j_1 dan j_2 adalah konjugat modulo n dan jika j_1 dan j_2 berderajat d, maka $2^s j_1 \equiv j_2 \ (mod\ n)$ dengan $s \in \{0,1, \dots, d-1\}$, sehingga $2^s j_1 mod\ n = j_2$. Untuk membuktikan $\mathcal{P}_{j_1}$ dan $\mathcal{P}_{j_2}$ adalah konjugat di $GF(2^m)$, maka akan ditunjukkan $\mathcal{P}_{2^s j_1 \bmod n} = \mathcal{P}_{j_2}^{2^s}$. Dengan menggunakan lemma 3.5.2 untuk menghitung $\mathcal{P}_{j_2}^{2^s}$ maka akan diperoleh:

$$\begin{aligned}\mathcal{P}_{j_2}^{2^s} &= \left(\sum_{i=0}^{m-1} P_{2^i j_2}^{2^{m-i}} \right)^{2^s}\\ &= \sum_{i=0}^{m-1} P_{2^i j_2.}^{2^{m-i} 2^s} \end{aligned} \quad (2.5.10)$$

Karena $2^{m-i} 2^i j_2 \bmod n = j_2$, maka $2^{m-i} 2^i j_2 \equiv j_2 \ (mod\ n)$. Karena kongruensi bersifat transitif dan $2^S j_1 \equiv j_1 (mod\ n)$, maka $2^{m-i} 2^i j_2 \equiv j_1 (mod\ n)$, sehingga dengan mengalikan kedua ruas dengan 2^s diperoleh:

$$2^{m-i} (2^s 2^i j_2) \equiv 2^s j_1 \ (mod\ n). \quad (2.5.11)$$

Dari (2.5.11) diperoleh:

$$\mathcal{P}_{j_2}^{2^s} = \sum_{i=0}^{m-1} P_{2^i j_2}^{2^{m-i} 2^s} = \sum_{i=0}^{m-1} P_{2^s 2^i j_2}^{2^{m-i}} = \mathcal{P}_{2^s j_1},$$

dengan $2^s j_1$ dalam modulo n. ■

Teorema 2.5.1 (Dimensi Kode SSRS)

Diberikan himpunan J dan sebuah kode siklik RS $\mathbb{C}(n, k_0, d_0)$ atas $GF(2^m)$ yang didefinisikan sebagai $\mathbb{C}(J)$. Misalkan S adalah subruang berdimensi v dari

$GF(2^m)$ yang direntang oleh basis $\{\beta_0, \beta_1, \dots, \beta_{v-1}\}$ dan $S^{\perp}$ adalah subruang trace-dual dari S berdimensi μ yang direntang oleh basis $\{\gamma_0, \gamma_1, \dots, \gamma_{\mu-1}\}$, dengan $\mu = m - v$. Misalkan r_j adalah rank matriks siklotomik ke-j, Γ_j. Dimensi biner kode $\mathbb{C}_S$, yang dinotasikan dengan $K(\mathbb{C}, S)$, adalah:

$$K(\mathbb{C}, S) = \sum_{j \in I_n} d_j (a_j - r_j) \qquad (2.6.2)$$

$$= \sum_{j \in I_n} (me_j - r_j d_j), \qquad (2.6.3)$$

dengan I_n = himpunan semua bilangan bulat terkecil pada setiap koset siklotomik modulo n,
d_j = banyaknya anggota koset siklotomik yang memuat j,
e_j = banyak bilangan bulat di $J_j = J \cap \Omega_j$, dengan Ω_j adalah koset siklotomik yang memuat j,
a_j = banyaknya bilangan bulat i sedemikian hingga $j2^i mod\ n \in J_j$,
m = bilangan bulat positif terkecil sedemikian hingga $n | 2^m - 1$.

Bukti:
Jika S adalah subruang $GF(2^m)$ yang direntang basis $B = \{\beta_0, \dots, \beta_{v-1}\}$, maka selalu dapat ditemukan basis untuk $GF(2^m)$ dari perluasan basis B dengan bentuk:

$$\mathfrak{B} = \{\beta_0, \beta_1, \dots, \beta_{v-1}, \beta_v, \dots, \beta_{m-1}\}.$$

Karena $\mathbb{C}$ adalah kode RS (n, k_0) atas $GF(2^m)$, maka $\mathbb{C}$ terdiri atas vektor-vektor $\boldsymbol{\mathcal{C}} = (\mathcal{C}_0, \mathcal{C}_1, \dots, \mathcal{C}_{n-1})$ dengan $\mathcal{C}_i \in GF(2^m), i = 0,1, \dots, n-1$. Jika $\mathcal{C}_i$ diekspansi menjadi m-tupel barisan biner yang bergantung pada basis $\mathfrak{B}$, maka berdasarkan definisi 2.4.1 kode SSRS adalah himpunan katakode $\mathbb{C}$ yang komponen binernya adalah nol jika berkorespondensi dengan $\{\beta_v, \dots, \beta_{m-1}\}$. Jika basis trace-dual untuk $S^{\perp}$ dinotasikan dengan $\mathfrak{G}_S = \{\gamma_0, \gamma_1, \dots, \gamma_{\mu-1}\}$, maka dapat dibentuk basis untuk $GF(2^m)$ dari perluasan basis $\mathfrak{G}_S$; yaitu, $\{\gamma_0, \gamma_1, \dots, \gamma_{\mu-1}, \gamma_\mu, \dots, \gamma_{m-1}\}$. Dengan menggunakan (2.1.5), maka kode SSRS dapat didefinisikan sebagai himpunan katakode $\mathbb{C}$ dengan bentuk $\boldsymbol{\mathcal{C}} = (\mathcal{C}_0, \mathcal{C}_1, \dots, \mathcal{C}_{n-1})$ yang memenuhi:

$$Tr_1^m(\gamma_h \mathcal{C}_i) = 0, \quad \begin{cases} h = v, v+1, \dots, m-1 \\ i = 0,1, \dots, n-1. \end{cases} \qquad (2.6.4)$$

Jika definisi kode SSRS dikombinasikan dengan polinomial MS yang didefinisikan di (2.4.4), maka didapatkan persamaan yang ekuivalen dengan (2.6.4) sebagai berikut:

$$Tr_1^m\left(\sum_{j \in J} (\gamma_h c_j x^j)\right) = 0, \begin{cases} h = 0,1,2, \dots \mu - 1 \\ x \in \{1, \alpha^{-1}, \alpha^{-2}, \dots, \alpha^{-(n-1)}\}. \end{cases} \qquad (2.6.5)$$

Kemudian didefinisikan polinomial $P_h(x)$ dan $\mathcal{P}_h(x)$ untuk $h = 0,1, \dots, \mu - 1$ sebagai berikut:

$$P_h(x) = \sum_{j \in J} \gamma_h c_j x^j \qquad (2.6.6)$$

$$\mathcal{P}_h(x) = Tr_1^m(P_h(x))\ mod\ (x^n - 1). \qquad (2.6.7)$$

$Tr_1^m(P_h(x)) = 0$ jika dan hanya jika $\mathcal{P}_h(x) = 0$ untuk $x \in \{1, \alpha, \dots, \alpha^{n-1}\}$. Berdasarkan lemma 2.5.1, $\mathcal{P}_h(x) = 0$ jika dan hanya jika

$$\mathcal{P}_{h,j} = 0 \quad \begin{cases} h = 0,1, \dots, \mu - 1 \\ j \in J, \end{cases} \qquad (2.6.8)$$

dengan $\mathcal{P}_{h,j}$ adalah koefisien x^j pada polinomial $\mathcal{P}_h(x)$. Dengan menggunakan lemma 2.5.2, didapatkan koefisien $\mathcal{P}_{h,j}$ sebagai berikut:

$$\mathcal{P}_{h,j} = \sum_{i=0}^{m-1} \gamma_h^{2^{m-i}} c_{j2^i}^{2^{m-i}},$$

dengan $j2^i$ dan 2^{m-i} dalam modulo n.
Karena kode SSRS adalah kode RS siklik $\mathbb{C}(J)$, maka bilangan bulat i pada $\mathcal{P}_{h,j}$ adalah bilangan bulat i sedemikian hingga $j2^i mod\ n \in J_j = J \cap \Omega_j$, sehingga

$$\mathcal{P}_{h,j} = \sum_{i \in A_j} \gamma_h^{2^{m-i}} c_{j.2^i}^{2^{m-i}}, \qquad (2.6.9)$$

dengan A_j adalah himpunan bilangan bulat i sedemikian hingga $j2^i mod\ n \in J_j = J \cap \Omega_j$.
Himpunan C_j yang elemen-elemennya adalah c_j dengan $j \in J$ bersesuaian dengan sebuah katakode di $\mathbb{C}_S$ jika dan hanya jika $\mathcal{P}_{h,j} = 0$ untuk setiap $h = 0,1, \dots, \mu - 1$ dan $j \in J$. Dengan menggunakan lemma 2.5.3, jika j_1, j_2 adalah konjugat modulo n atau j_1 dan j_2 berada di koset siklotomik yang sama dan $\mathcal{P}_{h,j_1}, \mathcal{P}_{h,j_2}$ juga konjugat di $GF(2^m)$, sehingga jika $\mathcal{P}_{h,j} = 0$ untuk satu elemen j dari koset siklotomik modulo n yang memuat j yang diberikan, maka koefisien semua elemen yang berada di koset siklotomik modulo n yang memuat j adalah nol. Oleh karena itu, ketika menghitung banyak koefisien himpunan C_j sedemikian sehingga $\mathcal{P}_{h,j} = 0$ cukup dengan membatasi j yang berada pada himpunan I_n. Jadi, untuk menghitung banyak himpunan C_j yang berkorespondensi dengan kode SSRS $\mathbb{C}_S$ sama dengan menghitung banyak solusi sistem persamaan yang berbentuk:

$$\sum_{i \in A_j} \gamma_h^{2^{m-i}} c_{j.2^i}^{2^{m-i}} = 0, \qquad h = 0,1, \dots, \mu - 1, j \in I_n. \qquad (2.7.1)$$

Misalkan N_j menyatakan banyak solusi pada sistem persamaan yang didefinisikan oleh (2.7.1). Karena sistem persamaan di (2.7.1) hanya melibatkan variabel-varibel pada c_l, dengan l adalah koset siklotomik ke-j, maka kita bisa menghitung banyak solusi sistem persamaan yang berkorespondensi pada tiap-tiap koset siklotomik secara terpisah. Ini berarti bahwa total banyak katakode di kode $\mathbb{C}_S$ yang dinotasikan dengan N_S diberikan oleh:

$$N_S = \prod_{j \in I_n} N_j. \qquad (2.7.2)$$

Teorema 2.5.1 akan terbukti jika kita bisa menunjukkan bahwa

$$N_j = 2^{me_j - r_j d_j} = 2^{d_j (a_j - r_j)}. \qquad (2.7.3)$$

Jika (2.7.3) terbukti, maka dimensi biner $\mathbb{C}_S$ adalah

$$K(\mathbb{C}, S) = \sum_{j \in I_n} K_j, \quad K_j = me_j - r_j d_j. \qquad (2.7.4)$$

Persamaan (2.7.1) dapat dinyatakan dalam bentuk matriks dengan menggunakan matriks siklotomik ke-j yang didefinisikan di (2.3.2), sehingga didapatkan:

$$\Gamma_j \boldsymbol{c}^T = \boldsymbol{0}^T, \quad (2.7.5)$$

dengan

$$\boldsymbol{c} = \left[c_{j.2^{i_0}}^{2^{m-i_0}}, c_{j.2^{i_1}}^{2^{m-i_1}}, \dots, c_{j.2^{i_{a_j-1}}}^{2^{m-i_{a_j-1}}}\right]. \quad (2.7.6)$$

Matriks Γ_j adalah matriks $\mu \times a_j$ dengan entri ke-(h,l) adalah $\gamma_h^{m-i_l}$. Jika $d \neq m$, maka ada e_j variabel berbeda pada vektor $\boldsymbol{c}$ dengan tiap-tiap variabel muncul f_j kali sebagai komponen $\boldsymbol{c}$. Karena pembahasan selanjutnya hanya membahas koset siklotomik ke-j maka indeks j dihilangkan pada a_j, d_j, e_j, f_j, sehingga a, d, e, f menyatakan a_j, d_j, e_j, f_j.

Ada 2 kasus; yaitu, $d = m$ dan $d \neq m$.

<u>Kasus 1. $d = m$</u>

Untuk $d = m$, semua komponen $c_{j.2^i}^{2^{m-i}}$ pada persamaan (2.7.6), dengan $i \in A_j$, adalah berbeda. Kemudian didefinisikan variabel x_l sebagai:

$$x_l = c_{j.2^{i_l}}^{2^{m-i_l}}, l = 0,1,\dots,e-1. \quad (2.7.7)$$

Karena pemetaan $\xi \to \xi^{2^{m-i_l}}$ adalah pemetaan satu-satu, maka $c_{j.2^{i_l}}$ dapat diperoleh kembali dengan tunggal dari x_l, sehingga dimensi $\mathbb{C}_S$ atas $GF(2)$ adalah dimensi ruang solusi sistem persamaan berikut:

$$\Gamma_j \boldsymbol{x}^T = \boldsymbol{0}^T, \quad (2.7.8)$$

dengan

$$\boldsymbol{x} = [x_0, x_1, \dots, x_{a-1}] = [x_0, x_1, \dots, x_{e-1}]. \quad (2.7.9)$$

Karena sistem persamaan pada (2.7.8) berupa persamaan polinomial atas $GF(2^m)$ yang membentuk ruang vektor atas $GF(2^m)$ dan juga merupakan persamaan linier homogen, maka himpunan solusi sistem (2.7.8) membentuk ruang solusi. Sehingga himpunan solusi sistem (2.7.8) adalah ruang vektor atas $GF(2^m)$ dan dimensi $\mathbb{C}_S$ atas $GF(2^m)$ adalah dimensi ruang solusi sistem persamaan (2.7.8) atau nolitas matriks Γ_j. Nolitas matriks Γ_j adalah $e - r$, dengan e adalah banyak variabel dan r adalah rank Γ_j. Jadi, banyak solusi sistem (2.7.8) adalah $(2^m)^{e-r} = 2^{me-dr} = 2^{d(a-r)}$.

<u>Kasus 2. $d \neq m$</u>

Untuk $d \neq m$, ada e komponen berbeda di $\boldsymbol{c}$ dengan tiap-tiap komponen muncul f kali. Karena indeks $i_l, l = 0,1,\dots,a-1$ di (2.3.1) diasumsikan berurutan naik, maka e komponen pertama $\boldsymbol{c}$ adalah berbeda dari yang lain dan pengulangan f kali di urutan yang sama, sehingga $\boldsymbol{c}$ dapat ditulis sebagai berikut:

$$\boldsymbol{c} = [\overbrace{c_{j.2^{i_0}}^{2^{m-i_0}}, c_{j.2^{i_1}}^{2^{m-i_1}}, \dots, c_{j.2^{i_{e-1}}}^{2^{m-i_{e-1}}}}^{e},$$

$$\overbrace{c_{j.2^{i_0}}^{2^{m-i_0-d}}, c_{j.2^{i_1}}^{2^{m-i_1-d}}, \dots, c_{j.2^{i_{e-1}}}^{2^{m-i_{e-1}-d}}}^{e}, \dots,$$

$$\overbrace{c_{j.2^{i_0}}^{2^{m-i_0-(f-1)d}}, c_{j.2^{i_1}}^{2^{m-i_1-(f-1)d}}, \dots, c_{j.2^{i_{e-1}}}^{2^{m-i_{e-1}-(f-1)d}}}^{e}]. \quad (2.8.1)$$

Karena d adalah derajat j, maka

$2^d j \equiv j(mod\ n) \leftrightarrow n|2^d j - j = n|j(2^d - 1) \leftrightarrow nk_1 = j(2^d - 1), k_1 \in \mathbb{Z}$.

Karena $n|2^m - 1$, maka $nk_2 = 2^m - 1,\ k_2 \in \mathbb{Z}$ sehingga

$$nk_2 = 2^m - 1$$
$$\frac{j(2^d-1)}{k_1} k_2 = 2^m - 1$$
$$j(2^d - 1)k_2 = k_1(2^m - 1)$$
$$(2^d - 1)(jk_2) = k_1(2^m - 1). \quad (2.8.2)$$

Dari (2.8.2) diperoleh $2^d - 1|2^m - 1$, sehingga $d|m$ dan $GF(2^d) \subseteq GF(2^m)$ dan $GF(2^m)$ dapat dipandang sebagai ruang vektor atas $GF(2^d)$ yang berdimensi $\frac{m}{d} = f$. Jika α adalah akar primitif $GF(2^m)$, maka $\{1, \alpha, \dots, \alpha^{f-1}\}$ adalah basis $GF(2^m)$ atas $GF(2^d)$ sehingga untuk sebarang $x \in GF(2^m)$ dapat dinyatakan secara tunggal sebagai:

$$x = \sum_{i=0}^{f-1} x_i \alpha^i,\ x_i \in GF(2^d).$$

Sehingga setiap koefisien $c_{j.2^i}^{2^{m-i}} \in GF(2^m)$ bisa diuraikan sebagai:

$$c_{j.2^{i_g}}^{2^{m-i_g}} = \sum_{l=0}^{f-1} x_{g,l} \alpha^l, \quad g = 0,1,\dots,e-1, \quad (2.8.3)$$

dengan $x_{g,l} \in GF(2^d)$ untuk semua $l = 0,1,\dots,f-1$.

Kemudian setiap komponen $\boldsymbol{c}$ akan diuraikan menjadi f variabel di sublapangan $GF(2^d)$. Karena $2^{kd} j \equiv j(mod\ n)$ dengan $k \in \mathbb{Z}^+ \cup \{0\}$, maka $2^i(2^{kd} j) \equiv 2^i j(mod\ n)$ dengan i yang memenuhi $2^i j(mod\ n) \in J_j$ adalah elemen A_j. Akibatnya, jika indeks i pada A_j, maka $i + d, i + 2d, \dots, i + (f-1)d$ juga di A_j sehingga jika $c_{i_g}^{2^{m-i_g}}$ di $\boldsymbol{c}$, maka:

$$c_{i_g}^{2^{m-i_g-d}}, c_{i_g}^{2^{m-i_g-2d}}, \dots, c_{i_g}^{2^{m-i_g-(f-1)d}}$$

juga di $\boldsymbol{c}$. Kemudian tiap-tiap bentuk $c_{i_g}^{2^{m-i_g}}, c_{i_g}^{2^{m-i_g-d}}, c_{i_g}^{2^{m-i_g-2d}}, \dots, c_{i_g}^{2^{m-i_g-(f-1)d}}$ dapat ditulis $c_{j.2^{i_g}}^{2^{m-i_g-ud}}$ dengan $u \in \{0,1,2,\dots,f-1\}$ diekspansi ke bentuk variabel $x_{g,l}$. Dengan menggunakan (2.8.3), maka didapatkan:

$$c_{j.2^{i_g}}^{2^{m-i_g-ud}} = \left[\sum_{l=0}^{f-1} x_{g,l} \alpha^l\right]^{2^{-ud}} \quad (2.8.4)$$

$$= \sum_{l=0}^{f-1} \left[x_{g,l} \alpha^l\right]^{2^{-ud}} \quad (2.8.5)$$

$$= \sum_{l=0}^{f-1} x_{g,l}^{2^{-ud}} \alpha^{l2^{-ud}} \quad (2.8.6)$$

dengan semua superskrip dan subskrip pada (2.8.4) – (2.8.6) dalam modulo n. Karena $x_{g,l} \in GF(2^d)$ dan $x_{g,l}^{2^{-ud}}$ adalah konjugat $x_{g,l}$ di $GF(2^d)$, maka $x_{g,l}^{2^{-ud}} = x_{g,l}$, sehingga

$$c_{j.2^{i_g}}^{2^{m-i_g-ud}} = \sum_{l=0}^{f-1} x_{g,l} \alpha^{l2^{-ud}} \quad u = 0,1,\dots,f-1. \quad (2.8.7)$$

Jika didefinisikan dua vektor; yaitu, $\boldsymbol{c}_g$ dan $\boldsymbol{x}_g$ dengan panjang f sebagai berikut:

$$\boldsymbol{c}_g = \left[c_{j.2^{ig}}^{2^{m-ig}}, c_{j.2^{ig}}^{2^{m-ig-d}}, \dots, c_{j.2^{ig}}^{2^{m-ig-(f-1)d}}\right] \quad (2.8.8)$$

$$\boldsymbol{x}_g = \left[x_{g,0}, x_{g,1}, \dots, x_{g,f-1}\right], \quad (2.8.9)$$

maka (2.8.7) bisa dinyatakan sebagai:

$$\boldsymbol{c}_g^T = V\boldsymbol{x}_g^T, \quad (2.9.1)$$

dengan V adalah matriks *Vandermonde* $f \times f$ yang didefinisikan sebagai berikut

$$V = \begin{bmatrix} 1 & \alpha^1 & \alpha^2 & \dots & \alpha^{(f-1)} \\ 1 & \alpha^{1.2^{-d}} & \alpha^{2.2^{-d}} & \dots & \alpha^{(f-1).2^{-d}} \\ 1 & \alpha^{1.2^{-2d}} & \alpha^{2.2^{-2d}} & \dots & \alpha^{(f-1).2^{-2d}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{1.2^{-(f-1)d}} & \alpha^{2.2^{-(f-1)d}} & \dots & \alpha^{(f-1).2^{-(f-1)d}} \end{bmatrix} \quad (2.9.2)$$

Karena $m = df$ dan α akar primitif $GF(2^m)$ serta V matriks nonsingular, maka himpunan elemen-elemen pada kolom kedua V; yaitu, $\alpha, \alpha^{2^{-d}}, \alpha^{2^{-2d}}, \dots, \alpha^{2^{-(f-1)d}}$, semuanya berbeda.

Kemudian didefinisikan 2 vektor, $\boldsymbol{c}'$ dan $\boldsymbol{x}$ sebagai berikut:

$$\boldsymbol{c}' = [\boldsymbol{c}_0, \boldsymbol{c}_1, \dots, \boldsymbol{c}_{e-1}] \quad (2.9.3)$$

$$\boldsymbol{x} = [\boldsymbol{x}_0, \boldsymbol{x}_1, \dots, \boldsymbol{x}_{e-1}]. \quad (2.9.4)$$

Karena matriks V di (2.9.2) tidak bergantung pada g, maka kita bisa menyatakan hubungan $\boldsymbol{c}'$ dan $\boldsymbol{x}$ pada (2.9.3) dan (2.9.4) sebagai:

$$\boldsymbol{c}'^T = W\boldsymbol{x}^T, \quad (2.9.5)$$

dengan W adalah matriks $a \times a$ sebagai berikut:

$$W = \begin{bmatrix} V & 0 & \dots & 0 \\ 0 & V & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & V \end{bmatrix}. \quad (2.9.6)$$

Vektor $\boldsymbol{c}$ yang didefinisikan di (2.7.6) dan vektor $\boldsymbol{c}'$ didefinisikan di (2.9.3) memiliki dimensi sama, misalkan a, dan komponen-komponen yang sama memiliki urutan yang berbeda. Dengan kata lain, kedua vektor dari $\boldsymbol{c}$ dan $\boldsymbol{c}'$ adalah permutasi satu sama lain. Karena sebarang permutasi vektor bisa dinyatakan dengan perkalian sebelah kiri dengan matriks permutasi nonsingular, misalkan Q, maka diperoleh:

$$\boldsymbol{c}^T = Q\boldsymbol{c}'^T. \quad (2.9.7)$$

Dengan mensubstitusikan (2.9.5) dan (2.9.7) ke (2.7.8), diperoleh:

$$\Gamma_j QW\boldsymbol{x}^T = \boldsymbol{0}^T, \quad (2.9.8)$$

sehingga banyak solusi sistem persamaan (2.7.5) sama dengan banyak solusi sistem (2.9.8) karena transformasi linier matriks nonsingular tidak mengubah dimensi ruang solusi. Karena sistem persamaan di (2.9.8) adalah himpunan μ persamaan linier pada a variabel yang berada di sublapangan $GF(2^d)$, maka banyaknya solusi adalah perpangkatan 2^d dan dimensi $\mathbb{C}_S$ atas $GF(2^d)$ adalah ruang solusi sistem (2.9.8) atau nolitas Γ_j; yaitu, $a - r$, sehingga total banyak solusi (2.9.8) adalah $2^{d(a-r)}$.

Jadi, dimensi biner untuk kode $\mathbb{C}_S$ adalah

$$K(\mathbb{C}, S) = \sum_{j \in I_n} d_j\left(a_j - r_j\right) = \sum_{j \in I_n} \left(me_j - r_j d_j\right). \blacksquare$$

3.6.1 CONTOH

Diberikan $\mathbb{C}\ (15, 7, 9)$ adalah kode siklik RS atas $GF(2^4)$, subruang $GF(2^4)$ adalah S yang direntang basis $\{1, \alpha\}$ dan diberikan himpunan $J = \{1,3,5,7,9,11,13\}$. Subruang trace-dual untuk $S^\perp = S$. Untuk menentukan dimensi kode $\mathbb{C}_S$, diberikan koset siklotomik modulo 15 pada contoh 2.2.3, larik siklotomik modulo 15, dan matriks siklotomik modulo 15.

Koset siklotomik modulo 15 adalah sebagai berikut:

$\Omega_0 = \{0\}$ $\quad d_0 = 1$ $\quad f_0 = 4$

$\Omega_1 = \{1,2,4,8\}$ $\quad d_1 = 4$ $\quad f_1 = 1$

$\Omega_3 = \{3,6,12,9\}$ $\quad d_3 = 4$ $\quad f_3 = 1$

$\Omega_5 = \{5,10\}$ $\quad d_5 = 2$ $\quad f_5 = 2$

$\Omega_7 = \{7,14,13,11\}$ $\quad d_7 = 4$ $\quad f_7 = 1$

dengan $I_{15} = \{0,1,3,5,7\}$.

Larik siklotomik modulo 15 adalah:

	Index i						
	0	1	2	3			
$j = 0$	0	0	0	0	$e_0 = 0$	$A_0 = \emptyset$	$a_0 = 0$
$j = 1$	**1**	2	4	8	$e_1 = 1$	$A_1 = \{0\}$	$a_1 = 1$
$j = 3$	**3**	6	12	**9**	$e_3 = 2$	$A_3 = \{0,3\}$	$a_3 = 2$
$j = 5$	**5**	10	**5**	10	$e_5 = 1$	$A_5 = \{0,2\}$	$a_5 = 2$
$j = 7$	**7**	14	**13**	**11**	$e_7 = 3$	$A_7 = \{0,2,3\}$	$a_7 = 3$

Matriks siklotomik untuk S adalah:

$$\Gamma_1 = \begin{bmatrix} 1 \\ \alpha \end{bmatrix}$$

$$\Gamma_3 = \begin{bmatrix} 1 & 1 \\ \alpha & \alpha^2 \end{bmatrix}$$

$$\Gamma_5 = \begin{bmatrix} 1 & 1 \\ \alpha & \alpha^4 \end{bmatrix}$$

$$\Gamma_7 = \begin{bmatrix} 1 & 1 & 1 \\ \alpha & \alpha^4 & \alpha^2 \end{bmatrix}.$$

Rank matriks $\Gamma_1, \Gamma_3, \Gamma_5$ dan Γ_7 adalah $r_1 = 1$, $r_3 = r_5 = r_7 = 2$

Dengan menggunakan teorema 2.5.1, dimensi biner $\mathbb{C}_S$ adalah

$$K(\mathbb{C}, S_1) = \sum_{j \in I_{15}} d_j\left(a_j - r_j\right) = 4(1-1) + 4(2-2) + 2(2-2) + 4(3-2) = 4,$$

atau

$$K(\mathbb{C}, S_1) = \sum_{j \in I_{15}} \left(me_j - r_j d_j\right) = (4.1 - 1.4) + (4.2 - 2.4) + (4.1 - 2.2) + (4.3 - 2.4) = 12 - 8 = 4,$$

sehingga didapatkan kode SSRS dengan parameter (15,2,14) atas S dan banyaknya katakode di $\mathbb{C}_S$ adalah $2^4 = 16$.

3. KESIMPULAN

Dari pembahasan diatas, diperoleh simpulan sebagai berikut:

1. Kode SSRS (*Subspace Subcode Reed-Solomon*) adalah salah satu kelas dari kode nonbiner RS (*Reed-Solomon*) $\mathbb{C}$

atas $GF(2^m)$ dengan parameter (n, k_0) yang berisi himpunan katakode $\mathbb{C}$ yang semua komponennya berada di subruang $GF(2^m)$ yang berdimensi v, misalkan S, yang dinotasikan dengan $\mathbb{C}_S$.

2. Misalkan dimensi $\mathbb{C}_S$ atas $GF(2)$ adalah $K(\mathbb{C}, S)$ dan $|\mathbb{C}_S|$ adalah banyaknya katakode di $\mathbb{C}_S$, maka $|\mathbb{C}_S| = 2^{K(\mathbb{C},S)}$ dan dimensi untuk $\mathbb{C}_S$ atas S adalah:

$$k(\mathbb{C}, S) = \frac{1}{v} K(\mathbb{C}, S) = {}^{|S|}\log|\mathbb{C}_S|.$$

Menggunakan teorema 2.5.1 diperoleh dimensi biner kode $\mathbb{C}_S$, yang dinotasikan dengan $K(\mathbb{C}, S)$, adalah:

$$K(\mathbb{C}, S) = \sum_{j \in I_n} d_j (a_j - r_j)$$
$$= \sum_{j \in I_n} (me_j - r_j d_j),$$

dengan I_n = himpunan semua bilangan bulat terkecil pada setiap koset siklotomik modulo n,

d_j = banyaknya anggota koset siklotomik yang memuat j,

e_j = banyak bilangan bulat di $J_j = J \cap \Omega_j$, dengan Ω_j adalah koset siklotomik yang memuat j,

a_j = banyaknya bilangan bulat i sedemikian hingga $j2^i \bmod n \in J_j$,

m = bilangan bulat positif terkecil sedemikian hingga $n|2^m - 1$,

sehingga banyaknya katakode di kode SSRS adalah

$$2^{\sum_{j \in I_n} d_j (a_j - r_j)} = 2^{\sum_{j \in I_n} (me_j - r_j d_j)}.$$

DAFTAR PUSTAKA

[1] Pretzel, Oliver. 1992. *Error-Correcting Codes and Finite Fields*. New York: Oxford University Press.

[2] Lint, J.H. Van. 1998. *Introduction to Coding Theory, Third Edition*. New York:Springer-Verlag Berlin Heidelberg.

[3] Pless, Vera. 1989. *Introduction to The Theory of Error Correcting Codes, Second Edition*. New York: John Wiley and Sons.

[4] Wicker, Stephen B. 1995. *Error Control Systems of Digital Communication and Storage*. New Jersey: Prentice-Hall, Inc.

[5] Wibisono, Gunawan dan Sari, Lydia. 2010. *Teknik Pengodean Sistem Komunikasi Dijital*. Bandung: Rekayasa Sains.

[6] Anton, Howard dan Rorres, Chris. 2004. *Aljabar Linear Elementer Versi Aplikasi* (Terjemahan). Jakarta : Penerbit Erlangga.

[7] Kholifah, Lia. 2012. *Konstruksi Kode LDPC (Low Density Parity Check) dari Koset Siklotomik*. Surabaya: UNESA(Tidak diterbitkan).

[8] Robinson, D.J.S. 2003. *An Introduction to Abstract Algebra*. Berlin: Walter de Grusyter.

[9] Lidl, Rudolf and Harald Niederreiter. 1994. *Introduction to Finite Fields and Their Applications*. United Kingdom : Cambridge University Press.

[10] Hersten, I. N. 1996. *Abstract Algebra,* 3nd Edition. New Jersey : Prentice Hall Internasional, Inc.

[11] Fraleigh, John B. 2000. *A First Course in Abstract Algebra*, 4th Edition. New York : Addison-Wesley Publising Company.

[12] Gallian, J.A. 1990. *Contemporary Abstract Algebra*, 2nd Edition. New York : Spgelangganger Science and Business Media, LLC.

[13] R. J. McEliece. 1987. *Finite Fields for Computer Scientists and Engineers*. Boston, MA: Kluwer.

[14] J. Gilbert, William and W. Keith Nicholson. 2004. *Modern Algebra with application*, 2nd Edition. Canada: John Wileyand Son, Inc.

[15] Hattorio, Masuksyuki dkk. 1998. *Subspace Subcodes of Reed-Solomon Codes,(Online)*,(http://authors.library.caltech.edu/6792/1/HATieeetit98.pdf diakses pada 26 September 2013).

[16] McEliece, R.J. dan Solomon, Gustave. 1994. *Trace-Shortened Reed-Solomon Codes,(Online)*, (http://tmo.jpl.nasa.gov/progress_report/42-117/117l.pdf diakses pada 16 Oktober 2013)